REMARKS

This amendment was filed with a Request for Continued Examination (RCE) pursuant to 37 CFR 1.114.

An interview between the applicant's agent and the Examiner was conducted by telephone on June 8, 2007. The substance of the interview was that further claim amendments proposed by the applicant would necessitate the filing of a RCE.

The applicant has carefully considered the Examiner's final rejection based on the cited prior art. The applicant submits that the claims as amended patentably distinguish the invention over the cited prior art for the following reasons:

There is no reasonable basis for a person of ordinary skill in the art to modify Mirov by Cooper

In the Detailed Action dated March 19, 2007 (the "Detailed Action"), the rejection of claims 1-2 and 6-13 under 35 U.S.C. 103(a) as being unpatentable over Mirov et al., U.S. Patent No. 6,138,236 ("Mirov") in view of Cooper et al., U.S. Patent No. 5,805,882 ("Cooper"), and the rejection of claims 4, 5 and 14-20 as being patentable over the allegedly admitted prior art in view of Mirov and Cooper, was maintained. The modification of Mirov by Cooper was supported by the identification of an alleged motivation to combine the cited references in Cooper, namely, that "[o]ne of ordinary skill in the art would have been motivated to make this modification [to modify Mirov with Cooper to include selective polling of a serial port based on a comparison of a key value] in order to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot. Mirov teaches that a comparison will fail if the flash ROM is corrupted (col. 4, lines 18-26)" (Detailed Action, page 5).

As a preliminary to the submissions regarding the pending claims as currently amended in this submission, the applicant respectfully submits that the obviousness rejection against the pending claims is improperly made because there is no reasonable basis to conclude that a person of ordinary skill in the art would combine Mirov and Cooper.

When rejecting claims as being obvious pursuant to 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 17 (1966). In addition, "'there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness'… [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ". *KSR Int'l Co.* v. *Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007), quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

However, while certain inferences may be drawn and while an obviousness analysis may not require the identification of precise teachings directed to the specific subject matter of the claims, the obviousness analysis should be set out explicitly, the analysis "cannot be sustained by mere conclusory statements", and the reason to combine the allegedly known elements should be "apparent". *Ibid.*

The teachings of Mirov are offered in a security context in which particular physical intervention is required before a boot PROM may be reprogrammed. Mirov teaches that changes may be effected by physically changing jumper settings or replacing old boot ROMs (column 1, lines 48-64). While Mirov describes these steps as time-consuming, Mirov teaches that safeguards are in place to prevent modification of the boot PROM (column 1, lines 38-46). Cooper, however, does not teach such a security concern. Having regard to the security contexts taught in Mirov and in Cooper, a person of ordinary skill in the art would infer that the modification of Mirov by Cooper would impact the security measures of Mirov in an undesirable manner; thus, exercising common sense, the skilled artisan would not consider modifying Mirov with Cooper's relaxed protocol regarding port access. The applicant submits that maintaining a combination of Mirov with Cooper in this manner is an impermissible use of the pending claims as a guide or roadmap in formulating the obviousness rejection.

Furthermore, in the Detailed Action it was noted that "Mirov does not explicitly disclose having a serial port and selectively polling the serial port for activity based on the result of the comparison" (Detailed Action, paragraph 6). In fact, Mirov does not disclose a serial or parallel port at all, which is not inconsistent with the security context disclosed in Mirov.

The claims as amended are patentable over the cited prior art

All independent claims have been amended. Claim 1, as amended, now reads:

> 1. A boot method for use in a mobile device having FLASH memory storing a key value and content comprising boot instructions stored in a security location, an internal read-only memory storing boot program code and a predetermined security value, and a serial port, execution of the boot program code stored in the read-only memory causing the mobile device to perform~~ing~~ the steps of:
>
> reading a key value from a security location in the FLASH memory, the key value being independent of the content of the FLASH memory;
>
> comparing the key value to a predetermined security value stored in the internal read-only memory, the predetermined security value being independent of the content of the FLASH memory; and
>
> depending on the result of the comparison of the key value to the predetermined security value, either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein.

By this amendment, claim 1 has been amended to specify that the FLASH memory stores both a key value and content comprising boot instructions and that the key value stored in the FLASH memory is independent of the content of the FLASH memory, and further that the predetermined security value is independent of the content of the FLASH memory.

Corresponding amendments have been made to the other independent claims, along with other tidying amendments. The following submissions apply equally to all currently pending claims, as presented in this amendment.

Although the applicant maintains that the reasoning for modifying Mirov with Cooper is improper, as set out above, the applicant further submits that the claims, as amended, are patentably distinguishable over Mirov as modified by Cooper for the reasons that: (1) neither reference, nor their combination, teaches the use of a key or security value that is *independent* of the content of flash memory; and (2) neither reference, nor their combination, teaches the use of a *predetermined* security value.

The prior art does not provide a key or security value* independent *of flash memory content

Turning first to Cooper, it is stated that "after the microcontroller boots up, the microcontroller checks the flash ROM contents by performing a check-sum of the flash ROM contents. If the checksum of the flash ROM contents matches an expected value..." (Cooper, col. 14, lines 38-42; see also col. 9, lines 30-46). The checksum of Cooper is thus a value that is derived from the contents of the flash ROM, and a value that is dependent on the contents of the flash ROM.

Similarly, Mirov provides only that:

> During initialization of the computer system 10, the secure micro-code 51 of the authentication section 45 executes and directs the hash generator 53 to generate a data hash of the unsecured micro-code 58 programmed in the programmable section 55 of the flash PROM 18. The secure micro-code 51 also directs the decryptor 54 to calculate a verification hash. The decryptor applies the public key 56 of the authentication section 45 and the digital signature 57 of the programmable section 55 and calculates the verification hash.
>
> Once the verification hash and the data hash are generated, the micro-code 51 directs the comparator 52 to compare the verification hash with the data hash. (Mirov, col. 4, lines 8-20)

Thus, Mirov and Cooper only teach a comparison or checking step, the outcome of which is dependent on the content of the code stored in flash memory. The applicant submits that unlike the subject matter of the currently amended claims, neither Mirov nor Cooper disclose the use of a key value or security value that is *independent* of the content of the flash memory. According to Cooper, the checksum is derived from the content of the flash ROM. A checksum is inextricably linked to the input from which the checksum is derived.

In the Advisory Action, it was stated that "Mirov teaches a key value that is independent form the contents of the FLASH memory because the key value does not depend on the contents of the FLASH memory (the signature is calculated using a public key that is independent of contents of PROM 18, figure 2 and col. 4, lines 18-41)." The applicant respectfully disagrees; a comparison to the public key of Mirov is inappropriate. As set out in the currently pending claims, the "key value" of this application itself is subject to the act of "comparing the key value to a predetermined security value stored in the internal read-only memory, the predetermined security value being independent of the content of the FLASH memory". Likening the public key of Mirov to the key value of the currently pending claims is of no assistance, because the public key of Mirov is not itself compared to another value. Rather, it is merely used in the process of calculating a verification hash. If the public key is relied on as providing the "key value" of the pending claims, then Mirov fails to teach a comparison involving such a "key value" at all, and also fails to disclose "comparing the key value to a predetermined security value stored in the internal read-only memory", as recited in claim 1. The values that *are* compared are hashes of the unsecured micro-code (Mirov, col. 4, lines 8-17). Being derived from the code, the hashes are inherently dependent, and not independent, on the content of the flash memory, contrary to the subject matter of the currently amended claims.

The prior art does not provide a* predetermined *security value

Furthermore, the applicant respectfully disagrees with the characterization of a verification hash as "predetermined". The common dictionary definition of "predetermine" is "to determine, decide, or establish in advance".[1] The explanation of a verification hash proffered in the Detailed Action, that a hash is predetermined because the result is predictable for a given, constant input (Detailed Action, page 13), is inconsistent with the normal meaning of "predetermined".

While a hash may always generate the same value given the same input, it does not follow that the hash is *predetermined.* The hash would only be predetermined if the hash, itself, were established in advance; this is not the case, because the hash itself is derived from another input. If the hash were truly predetermined, then it would not vary even if the input were altered; however, if the input is varied, the hash will consequently result in a different output. The hash is therefore not "predetermined", nor is it independent of the content from which it is derived. Similarly, a checksum is not "predetermined" or independent of the content from which it is derived, for the same reason.

For the forgoing reasons, the applicant submits that all currently pending claims are patentable

[1] The American Heritage® Dictionary of the English Language, Fourth Edition. Houghton Mifflin Company, 2004. Answers.com 19 Jun. 2007 < http://www.answers.com/topic/predetermine>.

over Mirov in view of Cooper. The subject matter of the claims provides a solution for enhancing the security of a mobile device in a manner not contemplated by Mirov or Cooper; indeed a person of ordinary skill in the art, even if motivated to combine Mirov and Cooper (which the applicant denies), would not arrive at the claimed subject matter, which provides for the comparison of values independent of the content of flash memory. The subject matter of the currently pending claims is directed to a system in which knowledge of checksums or digital signatures will not provide an advantage to a malicious user, unlike the cited prior art.

As described in the pending application and recited in the currently amended claims, there is a concern that a processor in a mobile device may be breached through a serial port line when a reset process is initiated, because upon reset the BootROM causes a serial port to be polled. If there is serial port activity, indicating that new code is to be downloaded, the BootROM will jump to a routine for downloading the new code; this new code may have complete access to other components in the mobile device (Application as published, paragraphs 4 and 5). It is therefore desirable to provide a "security feature" to reduce the likelihood of such a breach. (Application as published, paragraph 6). The present application therefore provides a security feature that comprises selective polling of the serial port, based on the result of a comparison between a value stored on an ASIC and a value stored in FLASH memory (Application as published, paragraph 8). The former value is a predetermined security value; the latter value is stored in a security location in FLASH memory (Application as published, paragraphs 8 and 9).

The "key value stored in the security location" and the "predetermined security value" recited in the claims thus provide a security feature that reduces the likelihood of a security breach in the manner described above; the serial port, as recited in the claims, is polled only if the recited security feature determines that it should be polled. This security feature is explicitly set out in the claims, which recite the "key value stored in the security location" and the "predetermined security value".

Mirov and Cooper, by contrast, are not directed to such a purpose. The step of calculating the checksum in Cooper is not directed to reducing the likelihood of a security breach by reducing the need for a port to be polled; it is directed to determining whether the FLASH memory has become corrupted (Cooper, col. 9, lines 30-46). Mirov, of course, is not directed to the polling of ports at all, let alone the possibility of a security breach by that means. The Applicant therefore submits that the claims as currently presented are patentable, as they are directed to a *security* measure to reduce security breaches via a serial port, whereas the cited art is not.

No new subject matter has been added by this amendment. Favourable reconsideration and allowance of this application are respectfully requested.

Executed at Toronto, Ontario, Canada, on June 19, 2007.

RICHARD C. MADTER
RYAN J. HICKEY
CHRISTOPHER PATTENDEN

Jenna L. Wilson
Registration No. 54908
(416) 971-7202, Ext. 290
Customer Number: 38735

JLW:lf